



Lindsay Nickle
1201 Elm Street
Suite 2550
Dallas, Texas 75270
lnickle@constangy.com
Direct: 248.709.9385

December 18, 2023

VIA ELECTRONIC SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Noteboom The Law Firm ("Noteboom") based in Hurst, Texas, in conjunction with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the Maryland data breach notification statute.

1. Nature of the Security Incident

On March 24, 2023, Noteboom discovered unusual activity in its digital environment. Following discovery, it immediately took steps to secure the network and engaged a dedicated team of external cybersecurity experts to assist in responding to and investigating the incident. As a result of the investigation, Noteboom learned that an unauthorized actor acquired certain files and data stored within its systems. Upon learning this, Noteboom launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, Noteboom confirmed on November 17, 2023, that personal information was contained in the affected data. Since that time, Noteboom has been working diligently to gather contact information and preparing to provide individual notice.

2. Type of Information and Number of Maryland Residents Notified

The data sets potentially acquired by the malicious actor(s) responsible for this incident included individuals' names, Social Security numbers or medical information. On December 18, 2023, Noteboom notified four (4) Maryland residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Noteboom has implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, Noteboom has offered individuals 12 months of complimentary services through CyberScout, a TransUnion company, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services, along with access to a call center for support for 90 days.

4. Contact Information

Noteboom remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at lnickle@constangy.com.

Very truly yours,

Lindsay Nickle of
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Encl: Sample Adult Consumer Notification Letter

Noteboom The Law Firm
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003



<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

December xx, 2023

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

Noteboom The Law Firm (“Noteboom”) is writing to inform you of a recent data security incident that may have involved your personal information. Noteboom takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your information, and offer you the opportunity to enroll in complimentary identity protection services that Noteboom is making available to you.

What Happened? On March 24, 2023, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. Upon learning this, we launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, we confirmed on November 17, 2023, that your personal information may have been involved in the incident. Since that time, we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

What Information Was Involved? Following our review of the contents of the impacted data, on November 17, 2023, we determined that your name and <<Custom Field 1>> were included. We emphasize that we have no evidence of any actual or attempted misuse of this information.

What Are We Doing? As soon as we discovered this incident, we took measures to further secure the network and enlisted outside cybersecurity experts to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information.

As a precaution, Noteboom is providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for <<service length>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [URL](#) and follow the instructions provided. When prompted please provide the following unique code to receive services: <<UNIQUE CODE>>

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What Can You Do? We encourage you to enroll in the complimentary services we are making available to you through Cyberscout. We also recommend that you review the guidance included with this letter about how to protect your information.

For More Information: If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the call specialist with your unique code listed above.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Charles M. Noteboom

Charles M. Noteboom, Esq.
Noteboom The Law Firm
669 Airport Freeway, #100
Hurst, TX 76053

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely over the next 12 to 24 months. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

**Washington D.C. Attorney
General**

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.